

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-084049

(43)Date of publication of application : 30.03.2001

(51)Int.Cl.

G06F 1/00

G06F 13/14

(21)Application number : 11-256243

(71)Applicant : CANON INC

(22)Date of filing : 09.09.1999

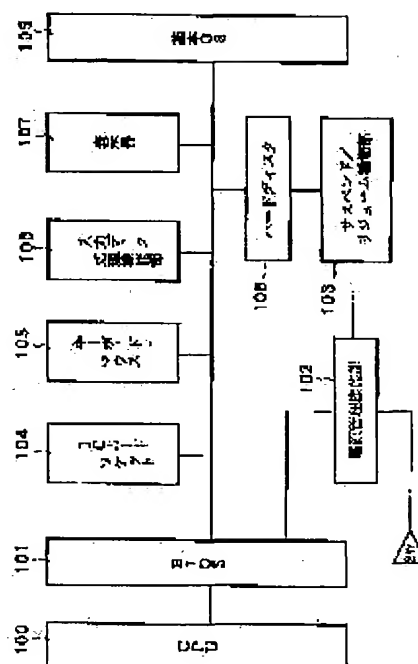
(72)Inventor : OKA KOJI

(54) COMPUTER AND SECURITY METHOD FOR COMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a computer and a computer security method capable of solving problems such as the processing load of a CPU and suitably protecting the computer.

SOLUTION: In the computer having an IC card socket 104 as a security device, a BIOS 101 judges whether the computer is to be protected or not on the basis of the inserted/ejected state of an IC card into/from the socket 104, and at the time of judging the necessity of protection, inhibits the processing of all or a part of hardware 105 or the like. Since the hardware 105 is directly controlled by the BIOS 101, the use of the computer body can be disabled and sure security measures can be applied to third persons.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-84049

(P2001-84049A)

(43) 公開日 平成13年3月30日 (2001.3.30)

(51) IntCl.⁷

識別記号

F I

テームト* (参考)

G 0 6 F 1/00

3 7 0

G 0 6 F 1/00

3 7 0 E 5 B 0 1 4

13/14

3 3 0

13/14

3 3 0 D

審査請求 未請求 請求項の数21 O L (全 16 頁)

(21) 出願番号

特願平11-256243

(22) 出願日

平成11年9月9日 (1999.9.9)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 岡 弘次

東京都大田区下丸子3丁目30番2号 キヤ

ノン株式会社内

(74) 代理人 100076428

弁理士 大塚 康徳 (外2名)

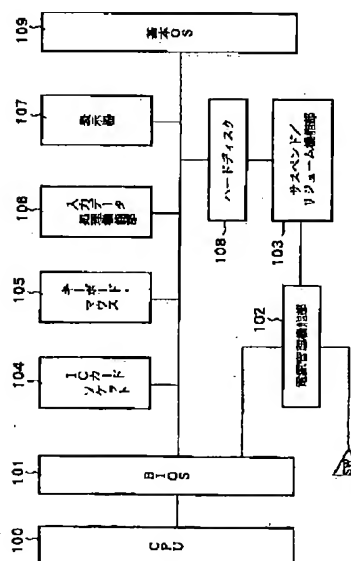
Fターム(参考) 5B014 HB04 HC03 HC06

(54) 【発明の名称】 コンピュータ及びコンピュータのセキュリティ方法

(57) 【要約】

【課題】 CPUの処理負担等の問題を解決し、コンピュータを好適に保護し得るコンピュータ及びコンピュータのセキュリティ方法を提供すること。

【解決手段】 セキュリティデバイスとしてのICカードソケット104を有するコンピュータであって、BIOS101が、ICカードソケット104に対するICカードの挿脱の状態に基づいて、コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、全部又は一部のハードウェア105等の処理を禁止する。BIOSによりハードウェアを直接コントロールすることで、コンピュータ本体を使用不能にすることを可能にし、第三者に対し強固なセキュリティ対策を施すことができる。



【特許請求の範囲】

【請求項1】 セキュリティデバイスを有するコンピュータであって、

前記コンピュータのBIOSが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウェアの処理を禁止することを特徴とするコンピュータ。

【請求項2】 前記セキュリティデバイスが、ICカードと当該ICカードを挿入するためのソケットと、からなり、

前記BIOSは、前記ICカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定することを特徴とする請求項1に記載のコンピュータ。

【請求項3】 前記BIOSは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウェアの処理を禁止することを特徴とする請求項1に記載のコンピュータ。

【請求項4】 前記BIOSは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止することを特徴とする請求項1に記載のコンピュータ。

【請求項5】 前記BIOSは、保護の必要があると判定した場合は、ディスプレイの表示を禁止することを特徴とする請求項1に記載のコンピュータ。

【請求項6】 前記BIOSは、保護の必要があると判定した場合は、電源のON/OFFを禁止することを特徴とする請求項1に記載のコンピュータ。

【請求項7】 前記BIOSは、前記ICカードが、前記ソケットに挿入されている場合は、電源のOFFを禁止することを特徴とする請求項2に記載のコンピュータ。

【請求項8】 セキュリティデバイスを有するコンピュータのセキュリティ方法であって、前記コンピュータのBIOSが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウェアの処理を禁止することを特徴とするコンピュータのセキュリティ方法。

【請求項9】 前記セキュリティデバイスが、ICカードと当該ICカードを挿入するためのソケットと、からなり、

前記BIOSは、前記ICカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定することを特徴とする請求項8に記載のコンピュータのセキュリティ方法。

【請求項10】 前記BIOSは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウェアの処理を禁止することを特徴とする請求項8に記

載のコンピュータのセキュリティ方法。

【請求項11】 前記BIOSは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止することを特徴とする請求項8に記載のコンピュータのセキュリティ方法。

【請求項12】 前記BIOSは、保護の必要があると判定した場合は、ディスプレイの表示を禁止することを特徴とする請求項8に記載のコンピュータのセキュリティ方法。

【請求項13】 前記BIOSは、保護の必要があると判定した場合は、電源のON/OFFを禁止することを特徴とする請求項8に記載のコンピュータのセキュリティ方法。

【請求項14】 前記BIOSは、前記ICカードが、前記ソケットに挿入されている場合は、電源のOFFを禁止することを特徴とする請求項9に記載のコンピュータのセキュリティ方法。

【請求項15】 セキュリティデバイスを有するコンピュータのBIOSのプログラムを記録した記憶媒体であって、該プログラムが、

前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウェアの処理を禁止するプログラムであることを特徴とする記憶媒体。

【請求項16】 前記セキュリティデバイスが、ICカードと当該ICカードを挿入するためのソケットと、からなり、

前記プログラムは、前記ICカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定するプログラムを含むことを特徴とする請求項15に記載の記憶媒体。

【請求項17】 前記プログラムは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウェアの処理を禁止するプログラムを含むことを特徴とする請求項15に記載の記憶媒体。

【請求項18】 前記プログラムは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止するプログラムを含むことを特徴とする請求項15に記載の記憶媒体。

【請求項19】 前記プログラムは、保護の必要があると判定した場合は、ディスプレイの表示を禁止するプログラムを含むことを特徴とする請求項15に記載の記憶媒体。

【請求項20】 前記プログラムは、保護の必要があると判定した場合は、電源のON/OFFを禁止するプログラムを含むことを特徴とする請求項15に記載の記憶媒体。

【請求項21】 前記プログラムは、前記ICカードが、前記ソケットに挿入されている場合は、電源のOF

Fを禁止するプログラムを含むことを特徴とする請求項16に記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デスクトップ及びノートブックパソコン、サーバーコンピュータ、若しくは同サーバーに接続するワークステーション等のコンピュータ機器に対するセキュリティシステムに関するものである。

【0002】

【従来の技術】第三者がコンピュータを無断で操作できないように、コンピュータのセキュリティシステムが提案されている。このセキュリティシステムでは、例えば、PCMCIAソケット或いは同様の専用ソケットをコンピュータに設け、そこにICカードが挿入されたか否かにより、正当な者の利用か否かを区別するものである。

【0003】そして、従来、ICカードによるセキュリティは基本的にはソフトウェアによる保護対策であり、例えばICカードが抜かれた場合に、あらかじめ定めた特定のアプリケーションを、ICカードに関連付けられたセキュリティソフトによって利用不可能にするか、同セキュリティソフトによって表示画面全体をモザイク化して判読不能する等のソフト処理を行うものである。

【0004】これらは、セキュリティ対象のアプリケーションとセキュリティソフトの仕掛けによって行われており、再度使用するにはカード挿入後にパスワードを入力し、操作者の正当性を認識しセキュリティソフトによる解除を行うようにしていたのが現状である。

【0005】

【発明が解決しようとする課題】しかしながら、上記従来の方法では、ICカードに関連付けられたソフトウェアを常時起動しておく必要性からメモリを常に占有されるという問題がある。また、ソフトによるICカードの抜き差しを定期的にソケットサービスプログラムに対し割り込み処理を使って発信することからCPUの負荷が大きくなり、その他の処理に遅延が発生するという問題がある。更に、特定のアプリケーションに対しての処理である為、パソコン本体は使用可能であり、その他のアプリケーションや資産は保護されていない等の問題がある。

【0006】従って、本発明の目的は、係る問題を解消し、コンピュータを好適に保護し得るコンピュータ及びコンピュータのセキュリティ方法を提供することにある。

【0007】

【課題を解決するための手段】本発明によれば、セキュリティデバイスを有するコンピュータであって、前記コンピュータのBIOSが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判

定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウェアの処理を禁止することを特徴とするコンピュータが提供される。

【0008】本発明においては、前記セキュリティデバイスが、ICカードと当該ICカードを挿入するためのソケットと、からなり、前記BIOSは、前記ICカードが前記ソケットに挿入されているか否かに基づいて、コンピュータを保護するか否かを判定することもある。この場合、前記BIOSは、前記ICカードが、前記ソケットに挿入されている場合は、電源のOFFを禁止することもできる。

【0009】また、本発明においては、前記BIOSは、作業中のデータを、所定の記憶手段に保存した後に、全部又は一部のハードウェアの処理を禁止することもできる。

【0010】また、本発明においては、前記BIOSは、保護の必要があると判定した場合は、キーボード又はマウスの入力を禁止することもできる。

【0011】また、本発明においては、前記BIOSは、保護の必要があると判定した場合は、ディスプレイの表示を禁止することもできる。

【0012】また、本発明においては、前記BIOSは、保護の必要があると判定した場合は、電源のON/OFFを禁止することもできる。

【0013】また、本発明によれば、セキュリティデバイスを有するコンピュータのセキュリティ方法であって、前記コンピュータのBIOSが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウェアの処理を禁止することを特徴とするコンピュータのセキュリティ方法が提供される。

【0014】また、本発明によれば、セキュリティデバイスを有するコンピュータのBIOSのプログラムを記録した記憶媒体であって、該プログラムが、前記セキュリティデバイスの状態に基づいて前記コンピュータを保護するか否かを判定し、保護の必要があると判定した場合は、前記コンピュータの全部又は一部のハードウェアの処理を禁止するプログラムであることを特徴とする記憶媒体が提供される。

【0015】

【発明の実施の形態】以下、本発明の好適な実施の形態について、図面を参照して詳細に説明する。

【0016】図1は、本発明の一実施形態に係るコンピュータのブロック図である。

【0017】図1のコンピュータは、CPU100、BIOS（基本入出力システム）101、電源管理機能部102、サスペンド／リジューム機能部103、セキュリティICカードを挿抜するソケット104、キーボード或はマウスポインタ等の入力機器105、入力データ

処理機能部106、表示器107、ハードディスク108、基本OS109を備える。なお、特に図示するものではないが、CPU100により参照、実行されるプログラムの配置される実行メモリ領域や、CPU100の作業領域、109基本OS、或いはOS上で動作するプログラム等が、データを一時的に格納する記憶メモリ領域等のRAM、外部記憶媒体はもちろん備えている。

【0018】図2は、ICカードコネクタとカードソケットの一般的な回路の例を示した図である。

【0019】図中、200はICカードコネクタ、201は接続信号線、202はカードソケット、203はソケット側の接続信号線、204は接続を認識し信号をhighに維持するVCC、205は割り込み信号線、206はリセット信号線、207はクロックリセット、である。

【0020】図2には明記していないが、ICカードがセキュリティカードか否かを判断する手段は、カードソケット及びICカードコネクタに専用の信号線を用意し、その信号線からの信号を認識する手段、或いはセキュリティ専用ソケットを用いても問題はなく、何ら限定するものではない。

【0021】以下、図2と図3とを用いてICカードの挿抜による信号の変化を説明する。図3は、ICカードの挿抜時のソケット104からの信号（以下、ソケット信号ともいう。）の状態と、電源管理機能部102が作動するタイミングを示した図である。

【0022】図3において、300はソケット202のカード認識による信号の変化を、301は割り込み信号の変化を、302はリセット信号の変化を、それぞれ示している。

【0023】操作者がICカードをタイミング300aで挿入した場合に、タイミング301aでVCCは信号をlowに落としカード認識を示す。割り込み回路は同信号を認識すると割り込み信号をhighにセットし、割り込み要求を出す。

【0024】割り込み要求により、任意の処理が実行された後、タイミング302aで割り込み信号をリセットし、チェックリセットは割り込み信号を落とす。

【0025】次に、タイミング300bで操作者がICカードを取り出すと、VCCは信号をhighにセットしカードの取りだしを認識する。同信号を認識すると、割り込み回路はタイミング301bで割り込み信号をhighにセットし、割り込み要求を出す。割り込み要求により、任意の処理が実行された後、タイミング302bで割り込み信号をリセットし、チェックリセットは割り込み信号を落とす。

【0026】次に、係る構成からなるコンピュータにおいて実行される処理について説明する。

<処理1>ここでは、ICカードの抜き差しによつて、全メモリ上の内容をHDDや所定のRAM上に設けられ

たサスペンド領域（退避領域）に格納し、パソコン本体を停止状態にする場合を述べる。図4および図5は、係る処理のフローチャートである。なお、この例では、セキュリティICカードが挿入された場合、ソケット信号をlowとし、非挿入時の同信号をhighとする。

【0027】まず、ICカードが抜かれると、ソケット信号がhighにセットされ（ステップS400）、ステップS401において割り込み信号をhighにセットして割り込み要求を出す。本実施形態では電源管理機能部102が割り込みを認識し、BIOS101に対しサスペンド処理のイベントを発する。

【0028】ステップS402では、BIOS101はイベントの発生によりサスペンド機能を起動し、全メモリ上のデータをHDD108上に設けた退避領域、或いは退避用に設けた専用RAM（図示しない）に保管し、ステップS403でサスペンドフラグをONにする。更に、ステップS404において割り込み回路で設定された信号をlowにリセットして電源を落とす。

【0029】次に、図5を参照して、ステップS500において電源が投入されると、ステップS501で電源管理機能部102は、ソケット信号を確認する。

【0030】ステップS502では、信号がhighかlowかを判定し、lowならばICカードが挿入されていると判断してステップS503で電源管理機能部102は割り込み信号をhighにセットし、BIOSに制御を渡す。highならばステップS500へ戻る。

【0031】次に、ステップS504において、BIOS101がイベント発生を感知したらサスペンドフラグを参照し、ONならばサスペンド状態であると判断しリジューム処理（復元処理）を行う。その後、サスペンドフラグをリセットし（ステップS505）、また、割り込み信号をリセット（ステップS506）して通常の処理へ至る。なお、特に明記はしないが、上記サスペンド及びリジューム処理例は、一般的な公知の方法で問題はない。

【0032】以上述べたようにICカードが抜かれた場合にパソコン自体を休止状態にすること、及び再度挿入された場合には休止状態以前の状態に復元することでパソコンを第三者に使用させることを禁止する効果があるばかりか、作業途中の状態を維持したまま保護対策を実施できる効果がある。

<処理2>この処理では、ICカードの抜き差しによつて、キーボード及びマウス等の入力機器105からのデータをコントロールすることによって、パソコン本体を使用不能状態にする場合を述べる。図6および図7は、係る処理のフローチャートである。

【0033】この例では、セキュリティICカードが挿入された場合のソケット信号をlowとし、非挿入時の同信号をhighとして述べる。

【0034】ICカードが抜かれると、ソケット信号が

highにセットされ(ステップS600)、割り込み要求を出す(ステップS601)。

【0035】ステップS602では、BIOS101が割り込みイベントの発生を認識し、入力データ処理機能部106に対しデータ取得を停止させる。これにより、キーボード・マウス105からの入力は、無効になる。その後、ステップS603において割り込み回路からの信号をリセットする。

【0036】次に、図7を参照して、ステップS700は、ICカードが挿入されたことを意味している。ステップS701では、VCCによる挿入信号を電源管理機能部102が認識し、ステップS702において、該信号をhighかlowかを判定する。lowであればステップS700へ戻り、highならば、ステップS703において、割り込み要求を出す。

【0037】BIOS101は、割り込みイベントを確認すると、ステップS704において入力データ処理機能部106に対しデータ取得処理を再開させる。これによりキーボード・マウス105からの入力が有効になる。その後、ステップS705で割り込み信号をリセットする。

【0038】以上述べたようにICカードが抜かれた場合にBIOSに対し、キーボードやマウスからの入力データ取得を停止し、再度挿入されている場合にのみ入力データを処理することでパソコン自体を使用不可能にし、第三者からの保護対策として効果がある。

<処理3>この例ではICカードの抜き差しによって、表示器への出力信号をコントロールし、表示画面を消しパソコン本体を使用不能にする場合を述べる。図8および図9は、係る処理のフローチャートである。なお、この例では、ICカードが挿入された場合のソケット信号をlowとし、非挿入時の同信号をhighとして述べる。

【0039】ICカードが抜かれると、ステップS800においてソケット信号がhighにセットされ、ステップS801で電源管理機能部102は割り込み信号をhighにセットし割り込み要求を出す。

【0040】ステップS802においてBIOS101は割り込みイベントの発生を認識し、図示しない表示機能部に対し表示器107への出力信号を停止させる。これにより、表示器107の表示内容が不変となる。その後、ステップS803で割り込み回路からの信号をリセットし、待機状態になる(ステップS804)。

【0041】次に、図9を参照して、ステップS900は、ICカードが挿入されたことを意味している。ステップS901で、ソケット信号が確認される。ステップS902において、ソケット信号がlowの場合はステップS900へ戻り、信号がhighの場合は、電源管理機能部102が割り込み信号をhighにセットし割り込み要求を出す(ステップS903)。

【0042】ステップS904では、BIOS101は割り込みイベントの発生を認識し、表示機能部に対し表示器107への信号出力を再開させる。これにより表示器107の表示内容が可変となる。その後、割り込み信号をリセットする(ステップS905)。

【0043】以上述べたようにICカードが挿入されている場合のみ、表示器への信号を出力するため、操作者がしばらくパソコンを放置する際に、ICカードを抜くだけで画面上の表示内容を消去し、第三者に対し保護対策としての効果がある。

<処理4>この例では、ICカードの抜き差しによって、電源管理機能部102をコントロールすることによって、ICカードが挿入された場合に電源が供給され、ICカードが挿入されている場合のみ電源の切断が行えるようにする場合を述べる。図10と図11は、係る処理のフローチャートである。この例では、セキュリティICカードが挿入された場合のソケット信号をlowとし、非挿入時の同信号をhighとして述べる。

【0044】ステップS1000は、コンピュータの電源が投入されたことを示している。ステップS1001では、カードソケット202がICカードの挿入を確認後、信号をlowにセットする。

【0045】ステップS1002では、電源管理機能部102はソケット信号がlowになるのを待ち、lowになった時点で電力を供給し、以降の通常のコンピュータ起動処理をBIOS管理下で行う(ステップS1003及びS1004)。即ち、ICカードが挿入されていることを認識したら電源を供給する。

【0046】次に、図11を参照して、ステップS1100は、電源の切断操作が行われたことを意味している。ステップS1101において、電源管理機能部102はソケット信号を参照し、ステップS1102においてlowを確認したら、ステップS1103で割り込み信号をセットし、システム終了(ステップS1105)及び割り込み信号のリセット(ステップS1106)の後、電源を遮断する。即ち、ICカードが挿入されていることを認識したら電源遮断を行う。その後、ステップS1106で割り込み信号をリセットする。

【0047】ここでICカードが抜かれている時点で電源の切断操作が行われた場合、ソケット信号(high)を認識したら、操作者にICカード挿入を要求するメッセージを出力することもできる(ステップS1104)。その方法は表示メッセージ或いは警告音や警告メッセージ等があるが何ら限定するものではない。

【0048】以上述べたようにセキュリティICカードが挿入されている場合にのみパソコンの使用を可能にし、パソコンを同ICカードを持たない第三者に使用させることを禁止する効果がある。

【0049】なお、上記処理4の例ではICカードの挿入時のみ、電源のON/OFFを行えるようにし、パソ

コンの使用を第三者に対し禁止する手段であったが、電源OFF後、ICカードの抜き忘れが発生し第三者に利用される不具合がある。

【0050】その対策として、ICカードが挿入された場合に電源が供給され、ICカードが抜かれている場合にのみ電源の切断が行えるようにする場合を述べる。図12は、係る処理のフローチャートである。この例では、ICカードが挿入された場合のソケット信号をlowとし、非挿入時の同信号をhighとして述べる。

【0051】ステップS1200は、電源の切断操作が行われたことを意味している。ステップS1201において電源管理機能部102はソケット信号を参照し、ステップS1202においてhighにセットされていることを認識した場合、すなわちICカードが抜かれていることを認識した場合は、ステップS1203において割り込み信号をhighにセットする。その後、システムの終了（ステップS1205）及び割り込み信号をリセット（ステップS1106）して、電源を遮断する。

【0052】ここでICカードが挿入されている時点で電源の切断操作が行われた場合、ソケット信号lowを認識したら、ステップS1204において電源管理機能部102は操作者にICカード取りだしを要求するメッセージを出力する。その方法は表示メッセージ或いは警告音や警告メッセージ等があるが何ら限定するものではない。

【0053】以上、本発明の好適な実施の形態について説明したが、上述した処理の例は、それぞれ組み合わせて用いることができることはいうまでもない。

【0054】なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能を実現される場合も含まれることは言

うまでもない。

【0055】

【発明の効果】以上説明したように本発明によれば、BIOSによりハードウェアを直接コントロールすることで、コンピュータ本体を使用不能にすることを可能にし、第三者に対し強固なセキュリティ対策を施すことができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンピュータの構成を示すブロック図である。

【図2】ICカードコネクタとカードソケットの一般的な回路の例を示した図である。

【図3】ICカードの挿抜時のソケット104からの信号の状態と、電源管理機能部102が作動するタイミングを示した図である。

【図4】本発明の一実施形態における処理1のフローチャートである。

【図5】本発明の一実施形態における処理1のフローチャートである。

【図6】本発明の一実施形態における処理2のフローチャートである。

【図7】本発明の一実施形態における処理2のフローチャートである。

【図8】本発明の一実施形態における処理3のフローチャートである。

【図9】本発明の一実施形態における処理3のフローチャートである。

【図10】本発明の一実施形態における処理4のフローチャートである。

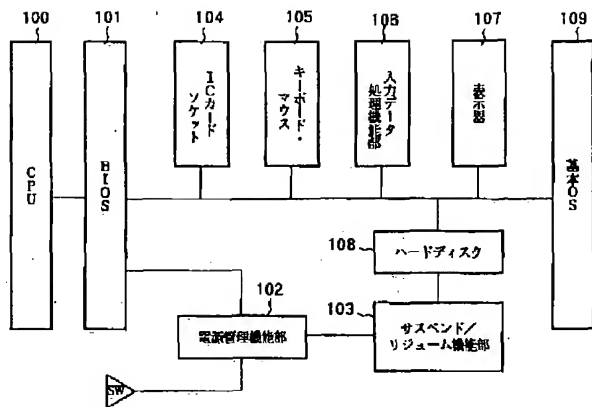
【図11】本発明の一実施形態における処理4のフローチャートである。

【図12】本発明の一実施形態における処理4のフローチャートである。

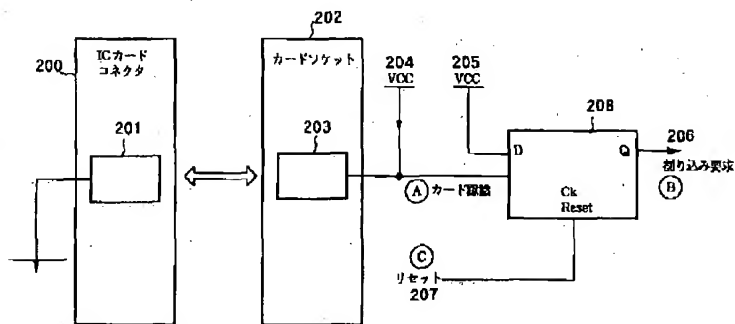
【符号の説明】

100 CPU
101 BIOS
102 機能部
103 サスペンド／リジューム機能部
104 ICカードソケット
105 キーボード或はマウス
106 入力データ処理機能部
107 表示器
108 ハードディスク
109 基本OS

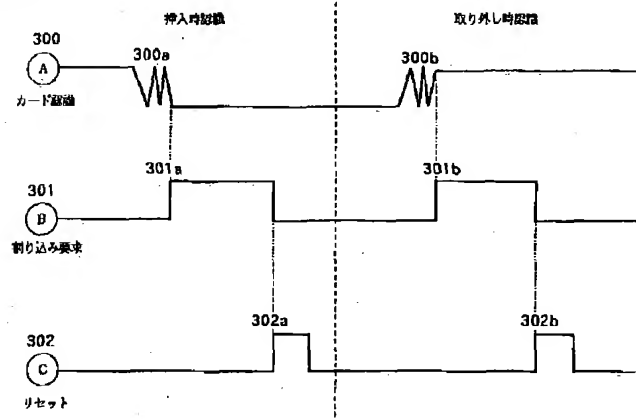
【図1】



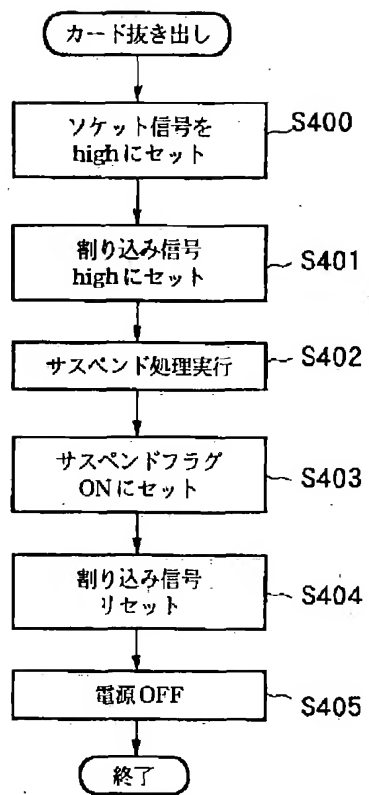
【図2】



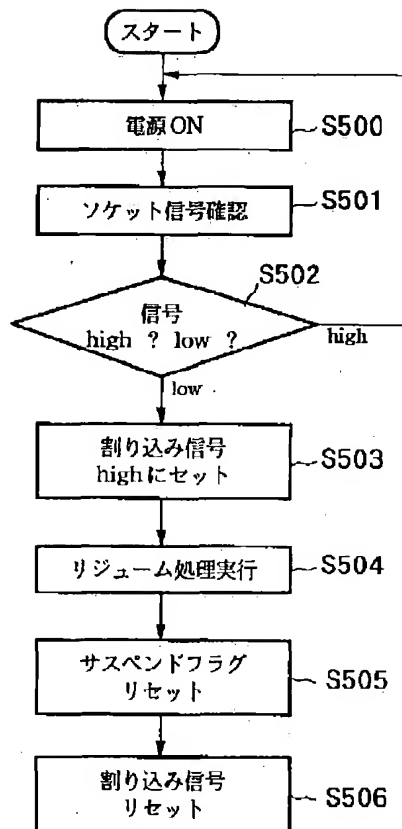
【図3】



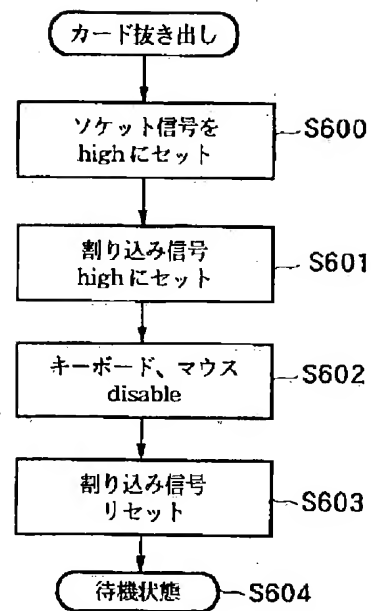
【図4】



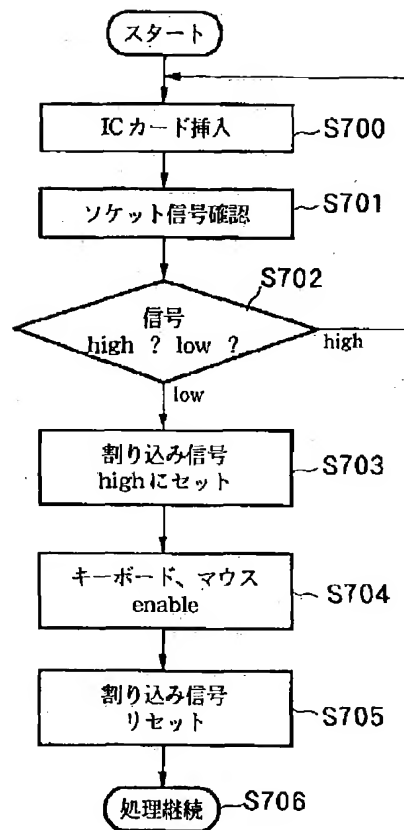
【図5】



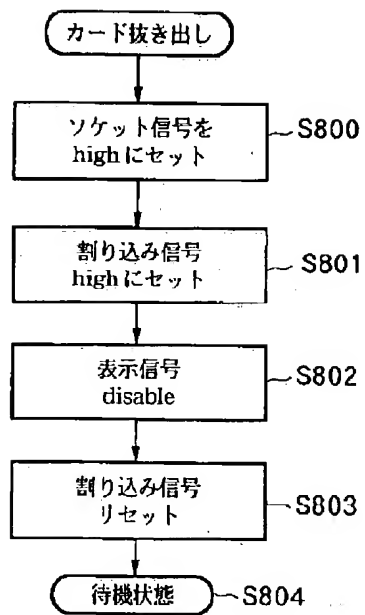
【図6】



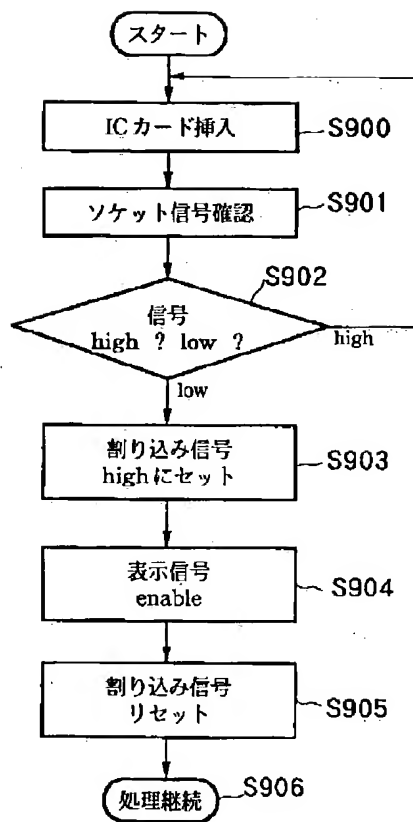
【図7】



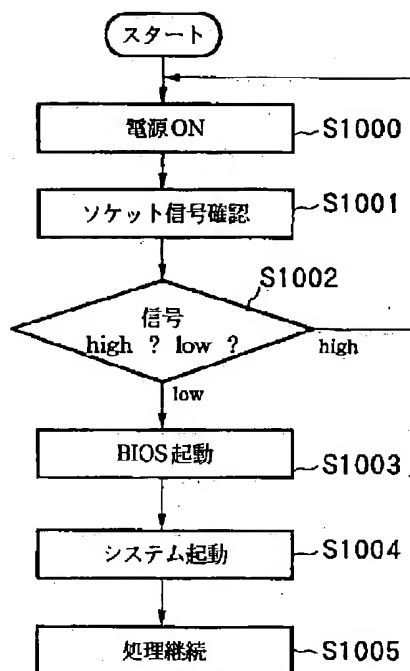
【図8】



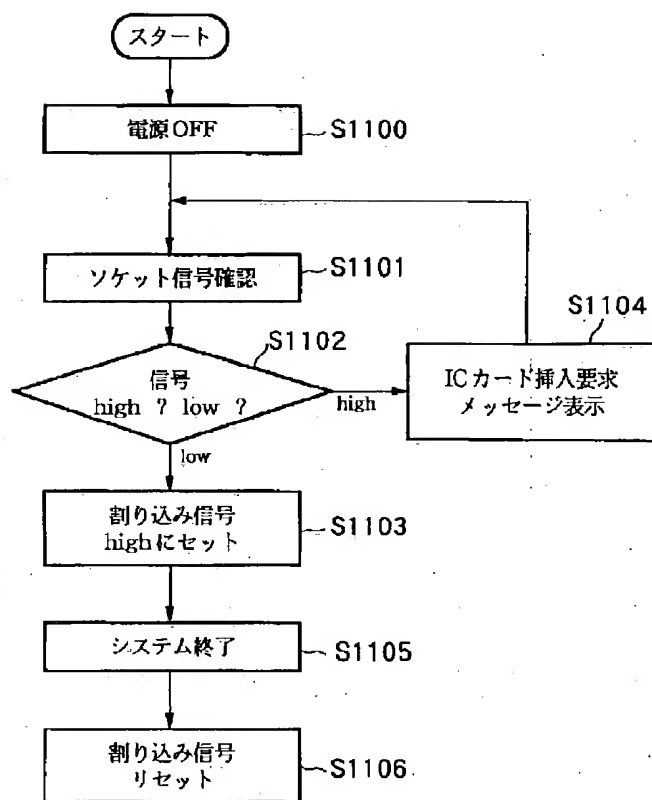
【図9】



【図10】



【図11】



【図12】

